世界知的所有権機関
国際事務局

PCT 特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 H04L 9/18, G09C 1/04	A1	(11) 国際公開番号	WO00/64096
		(43) 国際公開日	2000年10月26日(26.10.00)

(21) 国際出願番号 PCT/JP00/02554
(22) 国際出願日 2000年4月19日(19.04.00)
(30) 優先権データ
特願平11/147007 1999年4月19日(19.04.99) JP

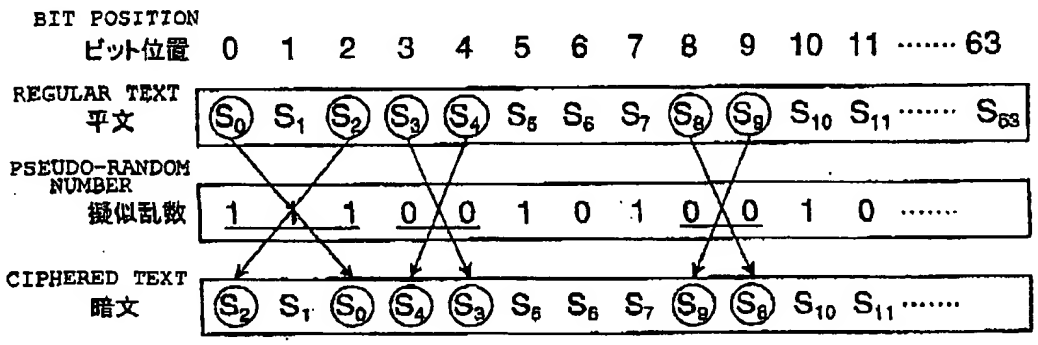
(71) 出願人；および
(72) 発明者
杉中順子(SUGINAKA, Junko)[JP/JP]
〒105-0001 東京都港区虎ノ門3-10-4 虎ノ門ガーデン408
Tokyo, (JP)
鈴木十士(SUZUKI, Toshi)[JP/JP]
〒362-0064 埼玉県上尾市小敷谷77-1
西上尾第二団地2-36-306 Saitama, (JP)
(71) 出願人（米国を除くすべての指定国について）
秋田靖夫(AKITA, Yasuo)[JP/JP]
〒105-0001 東京都港区虎ノ門3-10-4 虎ノ門ガーデン408
Tokyo, (JP)
(74) 代理人
小谷悦司, 外(KOTANI, Etsuji et al.)
〒550-0004 大阪府大阪市西区靭本町2丁目3番2号
住生なにわ筋本町ビル Osaka, (JP)

(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類
国際調査報告書

(54)Title: ENCRYPTED COMMUNICATION SYSTEM

(54)発明の名称 秘匿通信システム



(57) Abstract
An encrypted communication system for data communication in an encrypted status. A transmission device and reception device are provided with pseudo-random number sequence generating means for generating the same pseudo-random number sequence based on key information. The transmission device interprets a pseudo-random number sequence based on a preset transposition rule to thereby specify a plurality of exchange positions for a bit-string in a regular text; a ciphered text is prepared by exchanging individual values between these exchange positions. An example of a transposition rule is such that, in a portion of a pseudo-random number sequence where "1" or "0" continues over at least 2 bits, the leading bit and the trailing bit of each continuous portion are specified as a set of exchange positions to exchange bit values to each other.

(57)要約

データを秘匿状態として通信を行う秘匿通信システムである。送信側装置および受信側装置は、鍵情報に基づいて同一の疑似乱数列を生成する疑似乱数列生成手段を備える。送信側装置において、疑似乱数列を予め設定された転置規則に基づいて解釈することにより、平文のビット列に対して複数の交換位置が特定される。そして、これら交換位置の間でそれぞれの値が交換されることで暗文が作成される。転置規則の一例としては、疑似乱数列で２ビット以上にわたって１または０が連続する部分において、各連続部分の先頭ビット位置と後尾ビット位置とを交換位置の組として特定し、互いのビット値を交換する、という規則を挙げることができる。

明 細 書

秘匿通信システム

技術分野

本発明は、種々のデータを秘匿状態で通信する秘匿通信システムに関する。

背景技術

近年、種々のデータがインターネット等のネットワークを介して送受されている。その際、重要なデータが第三者に漏洩することを防止するため、送受するデータを秘匿状態とする種々の暗号化方法が提案されている。このような暗号化方法は、平文に対して、換字処理および転置処理を所定回数繰り返すことにより暗文を作成するものが多い。

しかしながら、従来の種々の暗号化方法においては、たとえば４ビット長や６ビット長等の所定ビット長を転置処理の単位とし、さらに予め定められたビット位置に対して転置処理が行われている。このため、従来の暗号化方法では、暗文に転置処理に起因する特徴が残ってしまい、解読されるおそれがあった。

本発明は、送受される暗文において、転置処理に起因する特徴を排除することができる秘匿通信システムを提供することを目的とする。

発明の開示

上記目的を達成するため、本発明にかかる秘匿通信システムは、所定の鍵情報に基づいて疑似乱数列を生成し、生成された疑似乱数列および予め設定された所

定の転置規則に基づいて、平文のビット列に対して複数の交換位置を特定し、これら複数の交換位置の間で互いの値を交換する転置処理を行うことにより、前記平文から暗文を作成し、この暗文を送信側装置と受信側装置とで送受することを特徴とする。

このような秘匿通信システムによれば、平文のビット列のうち、転置処理の対象となる交換位置が疑似乱数列に基づいて特定されるため、この交換位置は連続的に変化することとなる。したがって、送受される暗文において、転置処理に起因する特徴が排除され、高い暗号強度が得られる。

図面の簡単な説明

第１図は、本発明にかかる秘匿通信システムの全体概念図である。

第２図は、疑似乱数発生器の構成図である。

第３図は、疑似乱数列の一例を示す説明図である。

第４図は、平文のブロック化処理を示す説明図である。

第５図は、転置規則（１）に基づく暗号化処理（転置処理）の一例を示す説明図である。

第６図は、第５図に示した暗号化処理の概念図である。

第７図は、転置規則（１）に基づく復号化処理（転置処理）の一例を示す説明図である。

第８図は、ブロック化された平文の組立処理を示す説明図である。

第９図は、転置処理を複数回繰り返す暗号化処理の一例を示す説明図である。

第１０図は、転置処理を複数回繰り返す場合に、各回の転置処理に用いる疑似乱数列を、一連の疑似乱数列から抽出する処理を示す説明図である。

第１１図は、一連の疑似乱数列から複数の疑似乱数列を抽出する他の例を示す説明図である。

第１２図は、転置規則（２）に基づく暗号化処理（転置処理）の一例を示す説明図である。

第１３図は、転置規則（３）に基づく暗号化処理（転置処理）の一例を示す説明図である。

第１４図は、転置規則（４）に基づく暗号化処理（転置処理）の一例を示す説明図である。

第１５図は、転置規則（５）に基づく暗号化処理（転置処理）において、疑似乱数列から交換ビット位置の組を特定する処理の一例を示す説明図である。

第１６図は、転置規則（５）に基づく暗号化処理（転置処理）における交換処理を示す説明図である。

発明を実施するための最良の形態

第１図は、本発明にかかる秘匿通信システムの全体概略図である。

本発明にかかる秘匿通信システムは、インターネット等のネットワーク３０を介して接続可能な送信側装置１０および受信側装置２０とを備えている。

送信側装置１０は、所定の鍵情報４０に基づいて疑似乱数列を生成する疑似乱数列生成手段１１と、平文（原文）を所定ビット長のブロックに分割するブロック化手段１２と、平文の各ブロックに対し、前記疑似乱数列に基づいて後述する所定の転置処理を施すことにより平文から暗文を作成する暗号化手段１３と、作成された暗文をネットワーク３０を介して受信側装置２０に送信する送信手段１４とを備えている。

受信側装置２０は、前記暗文を受信する受信手段２２と、所定の鍵情報４０に基づいて前記送信側装置１０の疑似乱数列生成手段１１と同一の疑似乱数列を生成する疑似乱数列生成手段２１と、前記疑似乱数列に基づいて後述する所定の転置処理を施すことにより、暗文をブロックごとに復号化する復号化手段２３と、復号化された各ブロックを組み立てて平文（原文）を得る組立手段２４とを備えている。

なお、この実施形態においては、これら送信側装置１０および受信側装置２０は、パーソナルコンピュータ等によって構成され、上記各手段は、ソフトウェア

によって実現される機能ブロックとして構成されている。ただし、上記各手段の機能を果たすことができれば、上記各手段を専用回路等のハードウェアで構成することもできる。

また、送信側装置１０および受信側装置２０は、送信用または受信用の専用機である必要はなく、送信および受信とも可能な秘匿通信システムの送受信装置であることが望ましい。その際、後述するように、送信側用と受信側用に用いる疑似乱数列生成手段１１，２１等を、１つの手段で兼用することができる。

以下、各手段について、詳細に説明する。

疑似乱数列生成手段１１，２１は、送信側装置１０および受信側装置２０の両者ともに備えられており、両疑似乱数列生成手段１１，２１は、同一の構成である。このため、送信側装置１０および受信側装置２０の両機能を備えた送受信装置を構成する場合には、疑似乱数列生成手段１１，２１を兼用することができる。

疑似乱数列生成手段１１，２１は、具体的には、第２図に示す、一般にＭ系列と呼ばれる疑似乱数列を生成する回路に相当する機能を、コンピュータ上で実現するソフトウェアによって構成されている。この疑似乱数列生成手段１１，２１は、直列に接続されたｋ個のシフトレジスタx_1～x_kと、排他的論理和演算器ＸＯＲとの機能を果たす要素を備えており、各シフトレジスタx_1～x_kの出力のうち、フィードバック端子指定係数A_1～A_kによって指定された出力の排他的論理和が最上流側のシフトレジスタx_kの入力とされ、最下流側のシフトレジスタx_1からたとえば第３図に示す疑似乱数列が順次出力されるようになっている。

この疑似乱数列生成手段１１，２１によって生成される疑似乱数列は、どのシフトレジスタx_1～x_kからの出力の排他的論理和をとるかによって、疑似乱数列の系列が決定される。すなわち、上記フィードバック端子指定係数A_1～A_kが疑似乱数列の生成手順を示す情報となっている。

また、各シフトレジスタx_1～x_kに与えられる初期値X_1～X_kが、疑似乱数列のはじめのｋビット分の値、すなわち初期値となっている。

この秘匿通信システムでは、これらフィードバック端子指定係数A_1～A_kおよび疑似乱数の初期値X_1～X_kが鍵情報４０とされる。送信側装置１０および受信

側装置２０は、それぞれ、この鍵情報４０を操作者が入力するためのキーボード等の入力手段、あるいは、通信回線等によって入手する受信手段等を備えている。また、入力されたあるいは入手した鍵情報４０を記憶しておくメモリ等の記憶手段を備えている。疑似乱数列生成手段１１，２１は、こうして記憶手段に記憶された鍵情報４０を読み出して、鍵情報４０に基づいて疑似乱数列を生成するようになっている。

なお、疑似乱数列生成手段１１，２１は、鍵情報４０に応じて同一の疑似乱数列を再現できるものであれば、種々の公知の疑似乱数列生成手段を適用することができる。また、専用回路等のハードウェアで構成してもよい。

ブロック化手段１２は、第４図に示すように、送信側装置１０が受信側装置２０に送信する平文データを、所定ビット長（たとえば６４ビット長）のビット列からなるブロックに分割する処理を行う。平文データは、キーボード等の入力手段から入力されたデータでも、ハードディスク等の記憶手段から読み出したデータでもよい。

なお、平文データが所定ビット長に満たない場合は、任意のダミーデータを付加して所定ビット長のブロックを作成すればよい。

暗号化手段１３は、上記疑似乱数列生成手段１１によって生成された疑似乱数列を予め設定された転置規則に基づいて解釈することにより、ブロック化された平文のビット列に対して複数の交換位置を特定し、さらに、特定された複数の交換位置の間で互いの値を交換する転置処理を行う。

転置規則としては、後述するように、種々の規則を用いることができるが、この実施形態においては、次の転置規則（１）を採用する。

（１）疑似乱数列を２進数値列とし、この疑似乱数列で２ビット以上にわたって１または０が連続する部分において、各連続部分の先頭ビット位置と後尾ビット位置とを交換位置の組として特定し、互いのビット値を交換する。

暗号化手段１３は、このような転置規則を操作者が入力するためのキーボード等の入力手段、あるいは、通信回線等によって入手する受信手段等を備えている。

また、入力されたあるいは入手した転置規則を記憶しておくメモリ等の記憶手段を備えている。暗号化手段１３は、こうして記憶手段に記憶された転置規則を読み出して、転置規則に基づいて転置処理（暗号化処理）を行うようになっている。

第５図は、この転置規則（１）による転置処理の具体例を示す説明図である。この例は、平文は、６４ビット長を１ブロックとしたビット列S_0，S_1，S_2，…，S_{63}であり、各ビットには０または１のビット値が与えられている。疑似乱数列もまた、第３図に示すように、先頭ビットから６４ビットが用いられる。そして、疑似乱数列は、平文のビット列S_0，S_1，S_2，…，S_{63}と先頭ビットから１対１で対応させていく。

そして、上記転置規則（１）に基づいて、第５図の疑似乱数列を先頭ビットから順に解釈していけば、ビット位置０～２において、１が連続している。このため、この先頭ビットであるビット位置０とビット位置２とが交換位置の組として特定される。そして、平文のビット位置０のS_0とビット位置２のS_2とが互いのビット値を交換される。

同様に、疑似乱数列はビット位置３，４において０が連続し、ビット位置８，９において０が連続しているため、平文のS_3とS_4，S_8とS_9が、それぞれ互いのビット値を交換される。

以上の転置処理をビット位置６３まで行うことにより、６４ビット長の平文のビット列は、同じく６４ビット長の暗文のビット列に暗文化される。

なお、この第５図に示される転置処理は、第６図に示すように、いわゆる「あみだくじ」と同じ手順として模式的に表現することができる。すなわち、平文と暗文の対応するビット位置を縦線でつなぎ、交換位置の組の縦線同士を横線で接続した模式図を作成する。そして、この図において、平文の各ビット位置から縦線を下向きにたどり、横線の始点に到達すればその横線の終点が接続された縦線に移ることとすれば、暗文のあるビット位置に到達する。暗号化処理（転置処理）は、平文の各ビット位置のビット値を、上述のようにして到達した暗文のビット位置に書き込む処理となる。たとえば、平文の第０ビット位置のS_0は、横線によって、暗文の第２ビット位置に書き込まれることとなる。

このようにして、平文の第１ブロックの転置処理が終了すれば、第３図に示す

ように次の６４ビットの疑似乱数列を用いて平文の第２ブロックに対して上記と同様の転置処理を行われる。そして、このような転置処理を平文の全ブロックについて行うことにより、平文の全てが暗号化され、平文のブロックと同数の暗文のブロックが作成される。

送信手段１４および受信手段２２は、前記暗号化手段１３によって作成された暗文をネットワーク３０を介して送受する。具体的には、送信手段１４および受信手段２２は、ネットワーク上のプロトコル等に応じて、暗文に種々の情報を付加するソフトウェアおよびモデム装置等のハードウェアから構成される。なお、送信側装置１０および受信側装置２０の両機能を備えた送受信装置を構成する場合には、送信手段１４および受信手段２２は、両機能を備えた１つの送受信手段で実現することができる。

復号化手段２３は、上記疑似乱数列生成手段２１によって生成された疑似乱数列と、暗号化手段１３で用いられた転置規則とに基づいて、受信した暗文を復号化する復号化処理を行う。この実施形態では、暗文はブロック化されているため、各ブロックごとに、暗文のビット列を平文のビット列に復号化する。

具体的には、上記転置規則（１）によって転置処理が行われたこの実施形態では、第７図に示すように、上記転置規則（１）による転置処理と全く同じ処理によって、復号化処理を行うことができる。

復号化手段２３は、このような転置規則を操作者が入力するためのキーボード等の入力手段、あるいは、通信回線等によって入手する受信手段等を備えている。また、入力されたあるいは入手した転置規則を記憶しておくメモリ等の記憶手段を備えている。復号化手段２３は、こうして記憶手段に記憶された転置規則を読み出して、転置規則に基づいて転置処理（復号化処理）を行うようになっている。

なお、この復号化は、暗号化処理を模式的に表した第６図においては、暗文の各ビット位置から縦線を上向きにたどる処理となる。

したがって、送信側装置１０および受信側装置２０の両機能を備えた送受信装置を構成する場合には、上記暗号化手段１３を復号化手段２３として兼用するこ

とができる。

組立手段２４は、第８図に示すように、復号化手段２３によって復号化された複数のブロックに分割された平文を、一連の平文に組み立てる処理を行う。こうして組み立てられた平文は、モニタ等の出力手段に出力されるか、あるいは、ハードディスク等の記憶手段に書き込まれ、種々の用途に供される。

以上のような秘匿通信システムによれば、平文のビット列のうち、転置処理の対象となる交換位置が疑似乱数列に基づいて連続的に変化する。したがって、送受される暗文において、転置処理に起因する特徴が排除される。また、平文のビット列はビット単位で転置、攪乱されるため、高い暗号強度が得られる。

また、疑似乱数列に基づいて交換位置を特定し、交換位置のビット値を交換するだけの、簡単な処理で暗号化を行うため、暗号化処理および復号化処理の負担が小さく、高速化を図ることができる。

また、疑似乱数列の生成手順を特定する情報と疑似乱数列の初期値を示す情報とを鍵情報としているため、種々の疑似乱数列を生成することができ、この点からも高い暗号強度を得ることができる。

また、転置規則（１）によれば、交換位置がすべて同じ１ビット長であるから、暗号化手段１３および復号化手段２３を、同一の転置処理を行うものとして構成することができる。さらに、送信および受信の両方を行う送受信装置を構成する場合には、暗号化手段１３と復号化手段２３を１つの手段で兼用することができる。

また、転置規則（１）によれば、交換位置がすべて同じ１ビット長であるから、交換位置以外のビット位置の値は変化しない。したがって、転置処理において、交換位置以外のビット位置についてはバッファに記憶させることなく、直ちに暗文のビット列に書き込むことができ、転置処理を行う暗号化手段１３および復号化手段２３の処理負担を小さくすることができる。

また、２進数値の疑似乱数列を平文のビット列と１対１で対応させ、疑似乱数列に応じて交換位置が特定されるため、平文のビット列を先頭ビットから順に処

理していくことが可能である。したがって、暗号化された先頭ビットから順々に受信側装置２０に送出することができる。また、暗文の復号化も同様であるため、受信した暗文を先頭ビットから順に復号化処理することにより、送信側装置１０と受信側装置２０間で高いリアルタイム性を得ることもできる。

また、平文データを複数のブロックに分割し、各ブロックごとに暗号化し、復号化するため、暗号化処理および復号化処理が各ブロックごとに完結する。したがって、大容量の平文データに対しても、暗号化手段１３および復号化手段２３の負担を軽減することができる。

また、平文データを複数のブロックに分割するため、各ブロックごとに送受信処理を行うことができ、パケット通信方式等にも容易に対応できる。

次に、本発明にかかる秘匿通信システムの第２の実施形態について説明する。

この第２の実施形態は、暗号化手段１３が、平文の各ブロックに対して、転置規則（１）に基づく転置処理を複数回（３回）繰り返し行って、暗文化を行うものである。

上述したように、上記実施形態における転置処理を第６図の「あみだくじ」の手続きとして模式的に表せば、この第２実施形態における暗号化処理および復号化処理は、第９図に示すように、横線で表される転置処理を、複数段（３段）にわたって行う処理となる。

各転置処理には、疑似乱数列生成手段１１，２１が生成する疑似乱数列からそれぞれ切り出した異なる部分を用いればよい。具体的には、第１０図に示すように、疑似乱数列を先頭ビットから所定ビット長（たとえば６４ビット長）ごとのブロックに区切り、各ブロックを、第１ブロックの第１転置処理から順に用いればよい。あるいは、第１１図に示すように、疑似乱数列から、先頭ビット位置をｎビットずつずらして複数のブロックを抽出してもよい。

このように転置処理を複数回繰り返し行う構成とすれば、平文のビット列において、より多くのビット位置に対して容易に転置処理を施すことができる。

また、平文を所定ビット長のブロックに分割し、先頭ブロックから複数回（３回）の転置処理による暗号化処理を順次完結させていけば、暗号化処理が完了し

たブロックから順に送出することができるため、通信のリアルタイム性を高めることができる。

次に、本発明にかかる秘匿通信システムの第３の実施形態について説明する。

この第３の実施形態は、暗号化手段１３が、平文の各ブロックに対し、下記の転置規則（２）に基づく転置処理によって暗文化を行うものである。

（２）疑似乱数列を２進数値列とし、この疑似乱数列で０から１に変化する部分において、０に対応するビット位置と１に対応するビット位置とを交換位置の組として特定し、互いのビット値を交換する。

第１２図は、この転置規則（２）による転置処理の具体例を示す説明図である。上記転置規則（２）に基づいて、第１２図の疑似乱数列を先頭ビットから順に解釈していけば、ビット位置４，５において、０から１に変化している。このため、これらビット位置４とビット位置５とが交換ビットの組として特定される。そして、平文のビット位置４のS_4とビット位置５のS_5とが互いのビット値を交換される。同様にして、ビット位置６，７の組、およびビット位置９，１０の組においてビット値が交換され、暗文が作成される。

このように転置規則（２）によっても、平文のビット列における交換位置は疑似乱数列に応じて変化するため、転置処理に起因する特徴が排除された暗文をえることができる。

また、転置規則（２）によれば、交換位置がすべて同じ１ビット長であるから、暗号化手段１３および復号化手段２３を、同一の転置処理を行うものとして構成することができる。

なお、この転置規則（２）によって転置処理を行う場合であっても、上述した第２の実施形態のように、転置処理を複数回繰り返し行うことができる。以下の実施形態においても同様である。

次に、本発明にかかる秘匿通信システムの第４の実施形態について説明する。

この第４の実施形態は、暗号化手段１３が、平文の各ブロックに対し、下記の転置規則（３）に基づく転置処理によって暗文化を行うものである。

（３）疑似乱数列を２進数値列とし、この疑似乱数列で連続する１または０に対応するビット位置をそれぞれ一群の交換位置として特定し、隣り合う交換位置同士を群単位で交換する。

第１３図は、この転置規則（３）による転置処理の具体例を示す説明図である。上記転置規則（３）に基づいて、第１３図の疑似乱数列を先頭ビットから順に解釈していけば、ビット位置０～２は１が連続している。このため、ビット位置０～２は、同図でひとまとまりに囲っているように、一群の交換位置として特定される。つづいて、ビット位置３、４は０が連続している。このため、ビット位置３，４もまた、一群の交換位置として特定される。そして、平文のビット列において、これらビット位置０～２のS_0～S_2と、ビット位置３，４のS_3，S_4が、ビット群単位で交換される。

さらに、疑似乱数列において、ビット位置５では１が単独で存在する。このため、ビット位置５は１ビットで交換位置として特定される。同様に、ビット位置６では０が単独で存在する。このため、ビット位置６は１ビットで交換位置として特定される。そして、平文のビット列において、これらビット位置５のS_6と、ビット位置６のS_6とが交換される。

このような転置規則（３）によれば、平文のビット列における交換位置は疑似乱数列に応じて変化するため、転置処理に起因する特徴が排除された暗文を得ることができる。

特に、転置規則（３）によれば、転置処理の対象となる各交換位置のビット長が、疑似乱数に応じて変化するため、転置処理が多様化し、より一層暗号強度を高めることができる。

次に、本発明にかかる秘匿通信システムの第５の実施形態について説明する。

この第５の実施形態は、暗号化手段１３が、平文の各ブロックに対し、下記の転置規則（４）に基づく転置処理によって暗文化を行うものである。

（４）疑似乱数列を２進数値列とし、この疑似乱数列で連続する１に対応するビット位置をそれぞれ一群の交換位置として特定し、隣り合う交換位置同士を群単位で交換する。

第１４図は、この転置規則（４）による転置処理の具体例を示す説明図である。上記転置規則（４）に基づいて、第１４図の疑似乱数列を先頭ビットから順に解釈していけば、ビット位置０～２は１が連続している。このため、ビット位置０～２は、同図でひとまとまりに囲っているように、一群の交換位置として特定される。つづいて、疑似乱数列のビット位置５は１である。このため、ビット位置５が次の交換位置として特定される。そして、平文のビット列において、これらビット位置０～２のS_0～S_2と、ビット位置５のS_5が、群単位で交換される。

さらに、疑似乱数列のビット位置７およびビット位置１０は１である。このため、これらビット位置７およびビット位置１０は、それぞれ交換位置として特定される。そして、平文のビット列において、これらビット位置７のS_7とビット位置１０のS_{10}とが交換される。

このような転置規則（４）によっても、平文のビット列における交換位置は疑似乱数列に応じて変化するため、転置処理に起因する特徴が排除された暗文を得ることができる。

特に、転置規則（４）によれば、転置処理の対象となる各交換位置のビット長が、疑似乱数に応じて変化するため、転置処理が多様化し、より一層暗号強度を高めることができる。

次に、本発明にかかる秘匿通信システムの第６の実施形態について説明する。

この第６の実施形態は、平文の各ブロックに対し、下記の転置規則（５）に基づく転置処理によって暗文化を行うものである。

（５）疑似乱数列の各乱数値を平文のビット列のビット長未満の０を含む整数値とし、この疑似乱数列の先頭から２個ずつの各乱数値にそれぞれ対応するビット位置を平文のビット列における交換位置の組として特定し、各交換位置同士のビット値を交換する。

第１５図は、この転置規則（５）による転置処理を行うために用いられる疑似乱数列の具体例を示す説明図である。この実施形態では、平文をビット位置０～６３の６４ビット長からなるブロックとして扱うものとし、これに応じて、疑似乱数列の各乱数値は０～６３の整数値のいずれかをとる。疑似乱数列の各乱数値

は、平文のビット列における交換位置のビット位置を示す。そして、疑似乱数列の先頭から２個ずつの各乱数値が示すビット位置を交換位置の組とし、疑似乱数列のm個目までの乱数値を平文の第１ブロックの転置処理に用いる。

第１６図は、この転置規則（５）による転置処理の具体例を示す説明図であり、第１５図の疑似乱数列によって特定される第１番目の交換位置の組の交換（転置処理）を行う様子を示している。すなわち、第１５図の疑似乱数列では、第１の乱数値が６、第２の乱数値が１８であるから、ビット位置６とビット位置１８が交換位置の組として特定される。このため、平文のビット列において、ビット位置６のS_6と、ビット位置１８のS_{18}のビット値が交換される。

以下、疑似乱数列の先頭からm番目までの各乱数値について、同様の操作を行うことにより、第１のブロックについての暗文が作成される。なお、第２ブロックは疑似乱数列のm＋１～２m番目の各乱数値を用いて、第３ブロック以下も同様にして順次暗号化していけばよい。

このような転置規則（５）によっても、平文のビット列における交換位置は疑似乱数列に応じて変化するため、転置処理に起因する特徴が排除された暗文を得ることができる。

特に、転置規則（５）によれば、平文のビット列のなかで互いに離れたビット位置同士を交換位置の組とすることが容易であるため、転置処理が多様化し、より一層暗号強度を高めることができる。

以上、本発明を実施形態に即して説明したが、本発明にかかる秘匿通信システムは、上記実施形態に限定されるものではなく、以下のように構成してもよい。

（１）上記実施形態においては、転置規則（１）～（５）を挙げたが、転置規則はこれらに限定されない。すなわち、疑似乱数列に基づいて、平文のビット列に対し、複数の交換位置を一意に特定できる規則であれば、任意の転置規則を採用することができる。

（２）上記実施形態においては、平文を所定ビット長のブロックに分割してから暗号化処理を行ったが、このようなブロック化は必ずしも行う必要はなく、平文のビット列の先頭ビットから順次暗号化してもよい。

（３）上記実施形態においては、鍵情報として、Ｍ系列の生成手順を特定するフィードバック指定係数A_0～A_kおよび乱数初期値を用いたが、疑似乱数列を特定できる情報であれば、任意の情報を用いることができる。

（４）上記実施形態においては、送信側装置１０および受信側装置２０が備える疑似乱数列生成手段１１，２１をともに同一の構成からなる装置としたが、鍵情報に基づいて同一の疑似乱数を生成できるものであれば、任意の構成の疑似乱数生成手段１１，２１を用いることができる。

産業上の利用可能性

以上のように本発明によれば、ネットワークを介してデータを秘匿状態で送受する秘匿通信システムとして、疑似乱数列に応じて平文のビット列に対して転置処理を行うことにより、転置処理に起因する特徴を排除したシステムを提供することができる。

請求の範囲

1．データを秘匿状態として通信を行う秘匿通信システムであって、

送信側は、

所定の鍵情報に基づいて疑似乱数列を生成する疑似乱数列生成手段と、

生成された疑似乱数列および予め設定された所定の転置規則に基づいて、平文のビット列に対して複数の交換位置を特定し、これら複数の交換位置の間で互いの値を交換する転置処理を行うことにより、前記平文から暗文を作成する暗号化手段と、

前記暗文を送信する送信手段と、を備え、

受信側は、

前記暗文を受信する受信手段と、

前記所定の鍵情報に基づいて前記送信側の疑似乱数列生成手段と同一の疑似乱数列を生成する疑似乱数列生成手段と、

生成された疑似乱数列および前記転置規則に基づいて、受信した暗文を復号化する復号化手段と、を備えたことを特徴とする秘匿通信システム。

2．データを秘匿状態として通信を行う秘匿通信システムに用いられる送信側装置であって、

所定の鍵情報に基づいて疑似乱数列を生成する疑似乱数列生成手段と、

生成された疑似乱数列および予め設定された所定の転置規則に基づいて、平文のビット列に対して複数の交換位置を特定し、これら複数の交換位置の間で互いの値を交換する転置処理を行うことにより、前記平文から暗文を作成する暗号化手段と、

前記暗文を受信側装置に送信する送信手段と、を備えたことを特徴とする秘匿通信システムの送信側装置。

3．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記所定の鍵情報は、疑似乱数列の生成手順を特定する情報を含む秘匿通信シ

ステムの送信側装置。

4．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記所定の鍵情報は、疑似乱数列の初期値を示す情報を含む秘匿通信システムの送信側装置。

5．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記暗号化手段は、異なる疑似乱数列を用いて、前記転置処理を所定回数繰り返し行う秘匿通信システムの送信側装置。

6．請求の範囲第5項記載の秘匿通信システムの送信側装置において、

前記異なる疑似乱数列は、一連の疑似乱数列の異なる部分である秘匿通信システムの送信側装置。

7．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記転置処理は、疑似乱数列に応じて、平文のビット列に対して互いの値を交換する交換位置の組を特定し、各交換位置の組ごとに互いの値を交換するものである秘匿通信システムの送信側装置。

8．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記交換位置は、すべて同一ビット長からなる秘匿通信システムの送信側装置。

9．請求の範囲第8項記載の秘匿通信システムの送信側装置において、

前記交換位置は、すべて1ビット長である秘匿通信システムの送信側装置。

10．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記交換位置は、そのビット長が可変である秘匿通信システムの送信側装置。

11．請求の範囲第2項記載の秘匿通信システムの送信側装置において、

前記転置処理は、平文のビット列と２進数値の疑似乱数列とを先頭ビットから１対１で対応させ、疑似乱数列に予め設定された所定の特徴が認められるビット位置に対応する平文のビット位置を、前記交換位置として特定するものである秘匿通信システムの送信側装置。

１２．請求の範囲第２項記載の秘匿通信システムの送信側装置において、

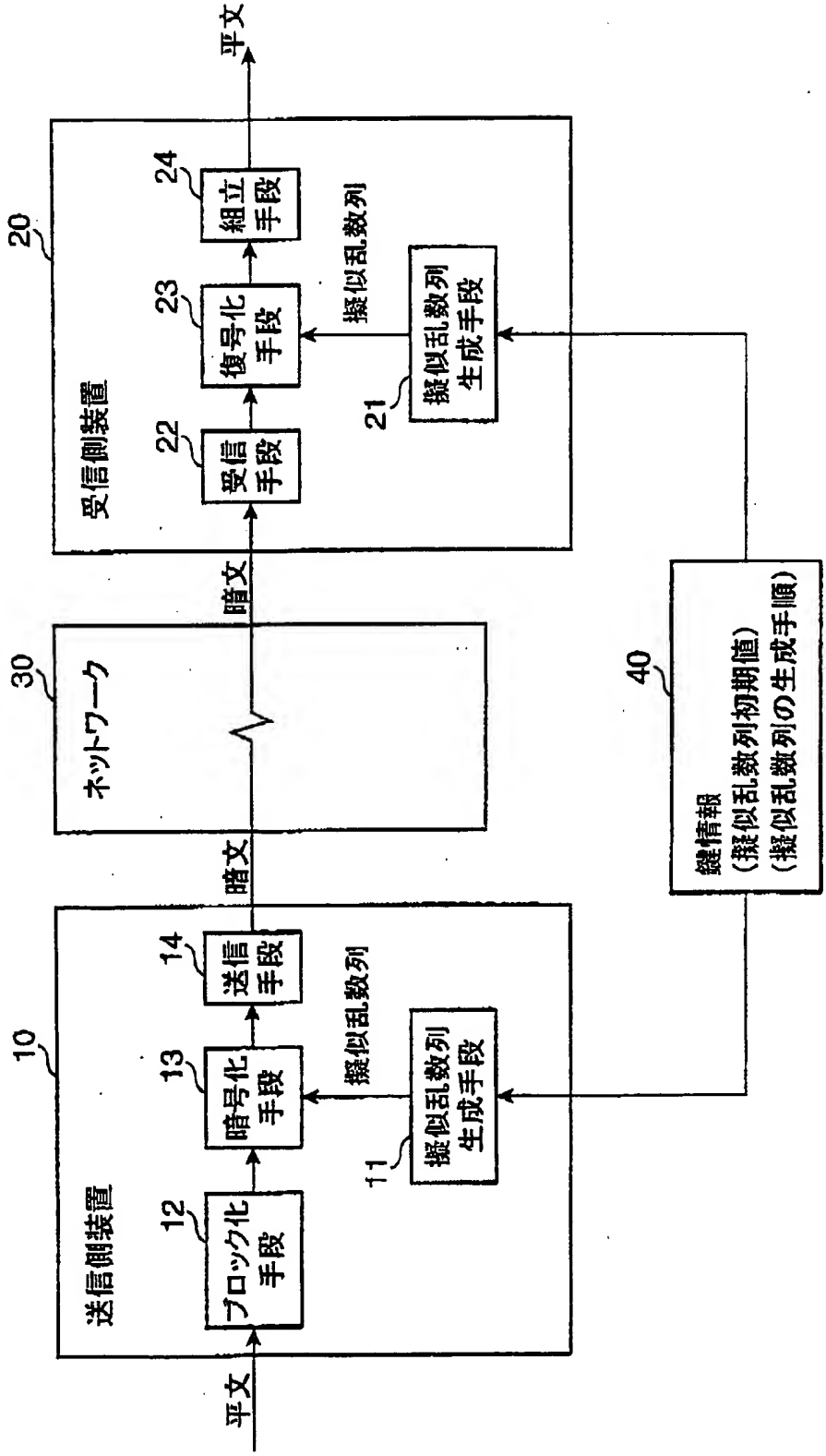
平文のビット列を所定ビット長のブロックに分割するブロック作成手段をさらに備え、前記暗号化手段は、各ブロック内で前記転置処理を行うものである秘匿通信システムの送信側装置。

１３．データを秘匿状態として通信を行う秘匿通信システムに用いられる送信側装置としてコンピュータを動作させるためのプログラムが記録されたコンピュータ読取り可能な記録媒体であって、

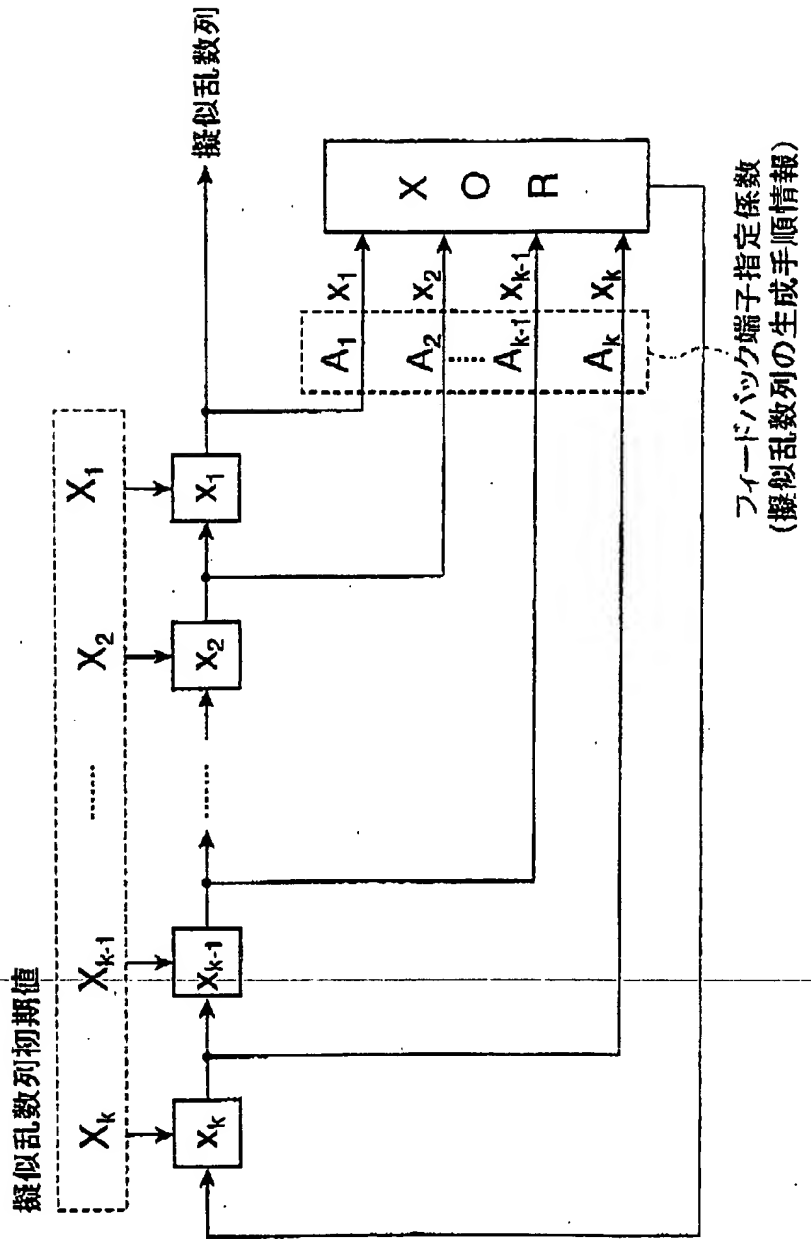
所定の鍵情報に基づいて疑似乱数列を生成する疑似乱数列生成機能と、

生成された疑似乱数列および予め設定された所定の転置規則に基づいて、平文のビット列に対して複数の交換位置を特定し、これら複数の交換位置の間で互いの値を交換する転置処理を行うことにより、前記平文から暗文を作成する暗号化機能と、をコンピュータに実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

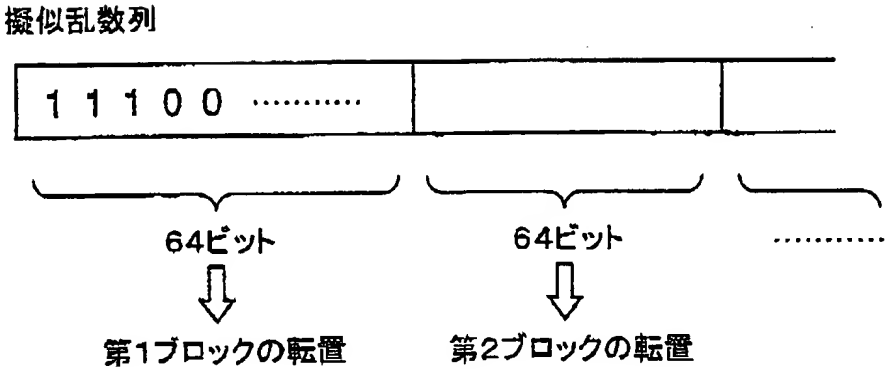
第１図


平文
送信側装置
10
ブロック化手段
12
暗号化手段
13
送信手段
14
擬似乱数列
擬似乱数列生成手段
11
暗文
ネットワーク
30
暗文
受信側装置
20
受信手段
22
復号化手段
23
組立手段
24
擬似乱数列
擬似乱数列生成手段
21
平文
鍵情報
(擬似乱数列初期値)
(擬似乱数列の生成手順)
40

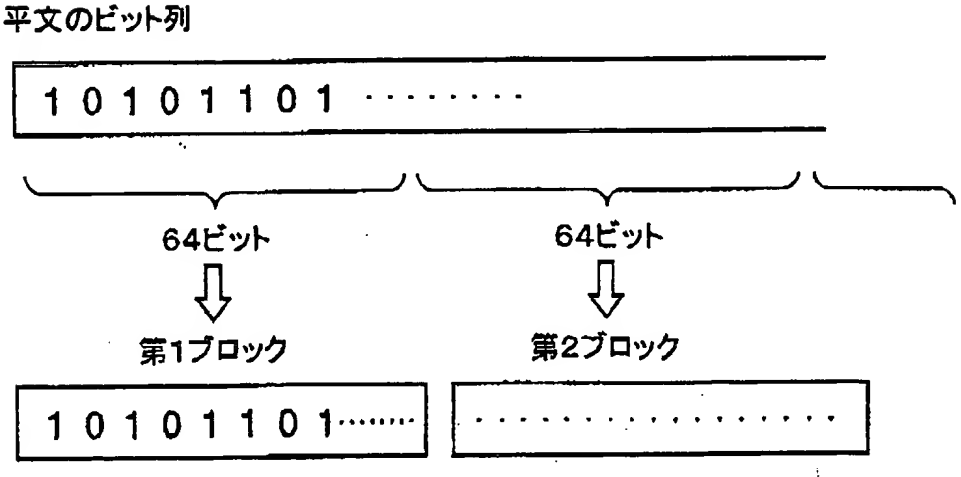
第２図



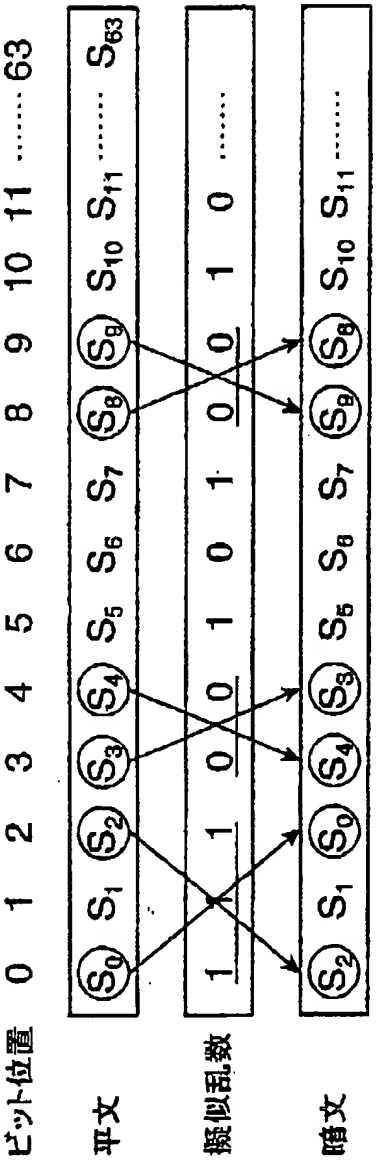
第 3 図


擬似乱数列
1 1 1 0 0 .....
64ビット
64ビット
.....
第1ブロックの転置
第2ブロックの転置

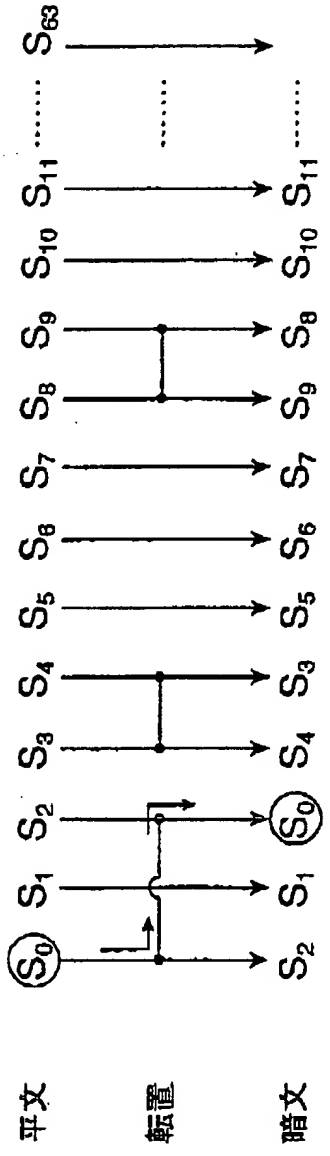
第 4 図


平文のビット列
1 0 1 0 1 1 0 1 .....
64ビット
64ビット
第1ブロック
第2ブロック
1 0 1 0 1 1 0 1.....
.....

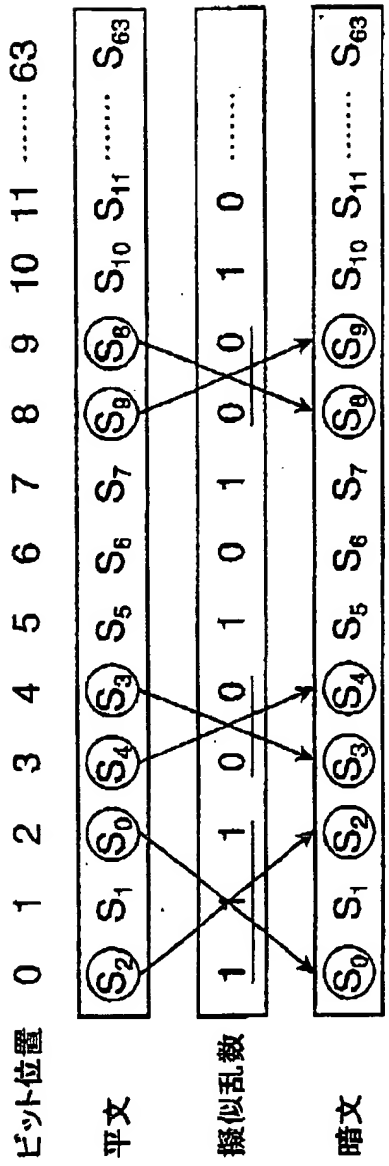
第５図



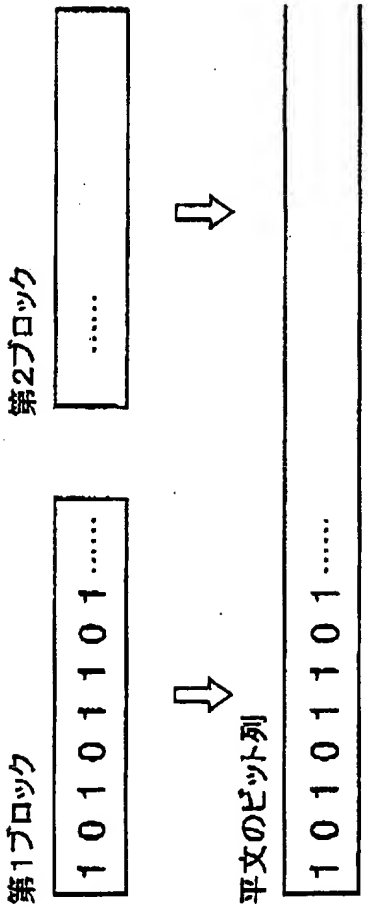
第６図



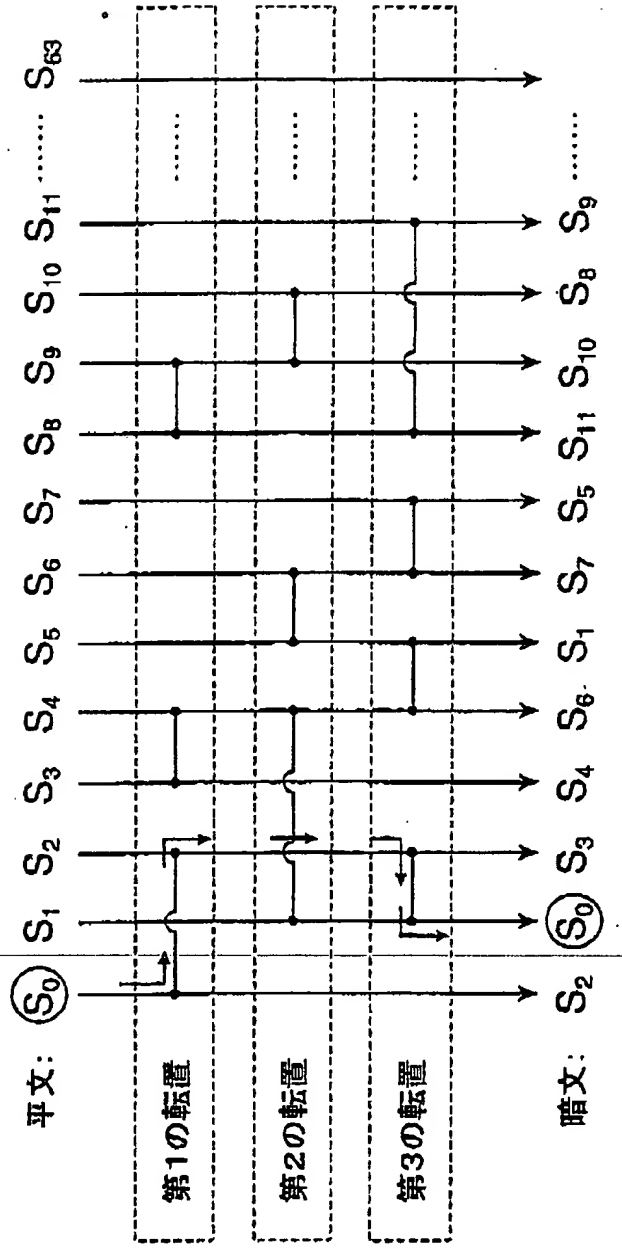
第７図


ビット位置 0 1 2 3 4 5 6 7 8 9 10 11 63
平文
擬似乱数
暗文
1 1 0 0 1 0 1 0 0 1 0 .....

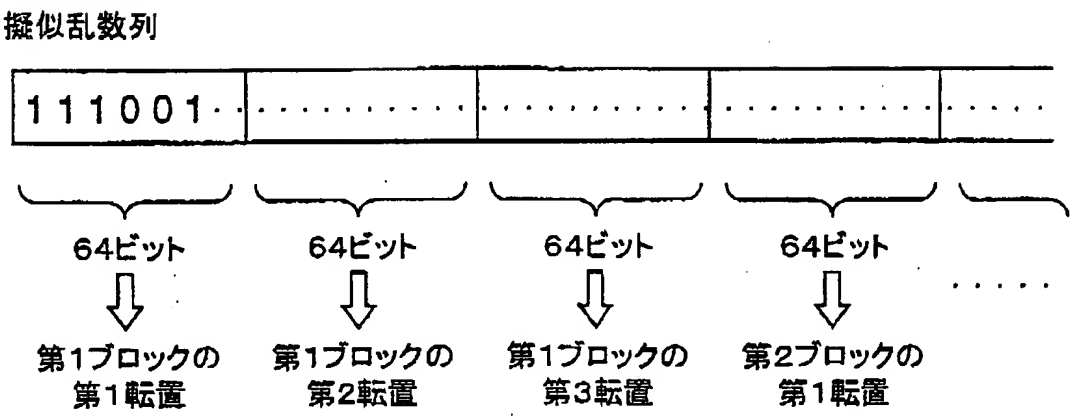
第８図


第1ブロック
第2ブロック
1 0 1 0 1 1 0 1 .....
.....
平文のビット列
1 0 1 0 1 1 0 1 .....

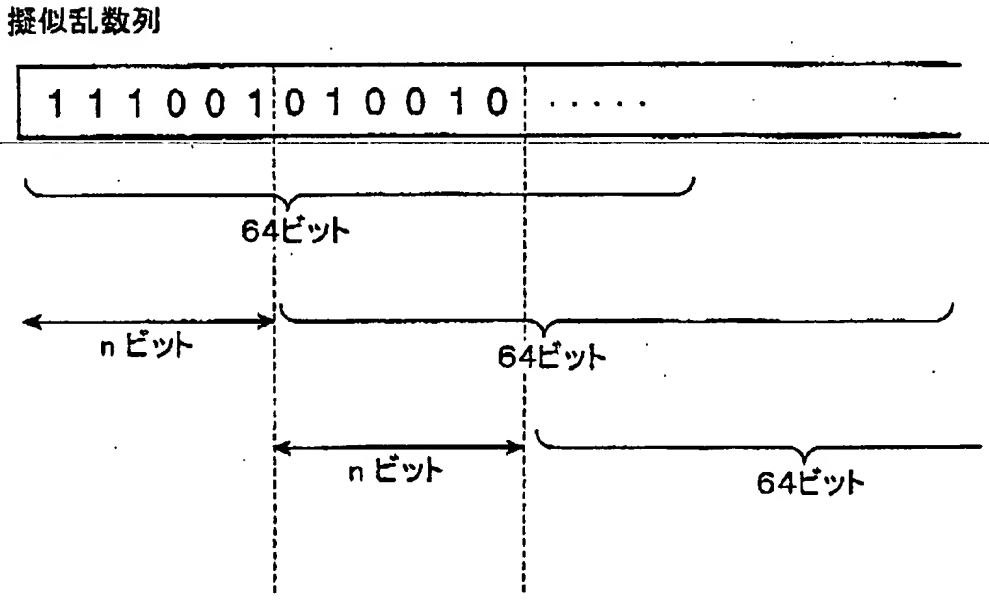
第９図



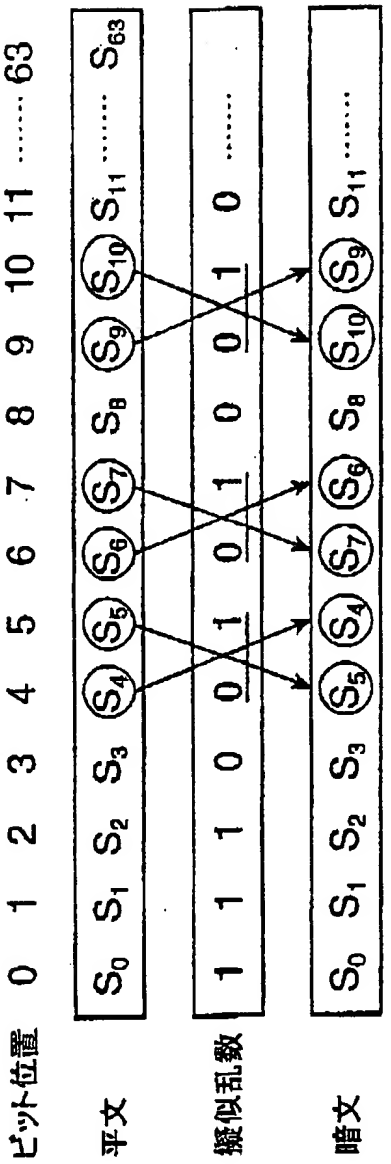
第 10 図


擬似乱数列
111001
64ビット
64ビット
64ビット
64ビット
第1ブロックの
第1転置
第1ブロックの
第2転置
第1ブロックの
第3転置
第2ブロックの
第1転置

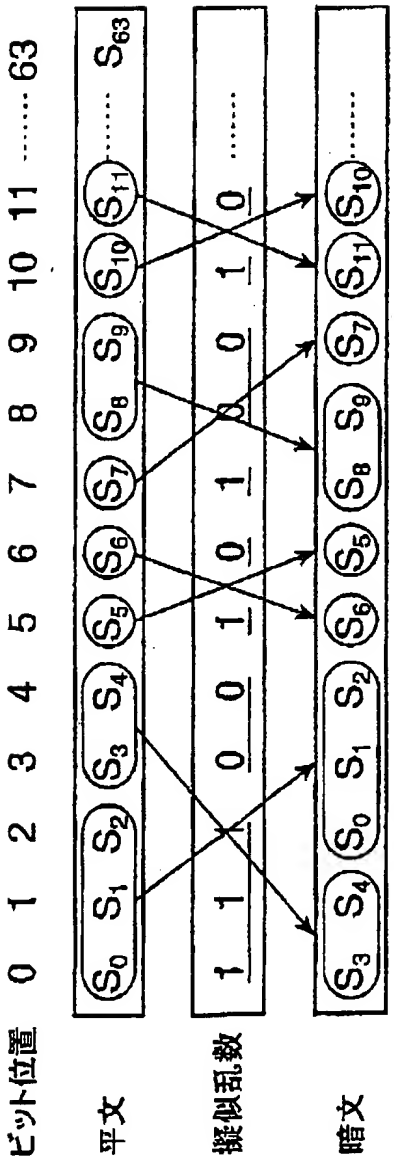
第 11 図


擬似乱数列
111001010010
64ビット
nビット
64ビット
nビット
64ビット

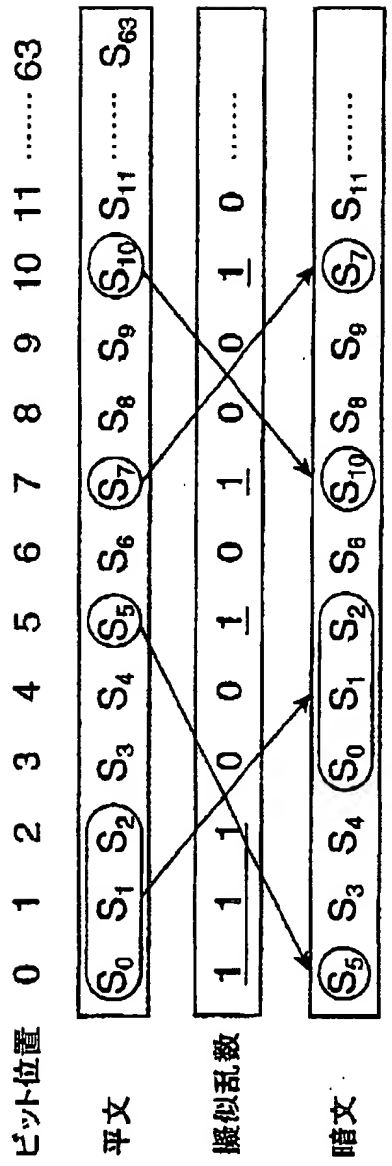
第12図


ビット位置 0 1 2 3 4 5 6 7 8 9 10 11 63
平文
擬似乱数
暗文

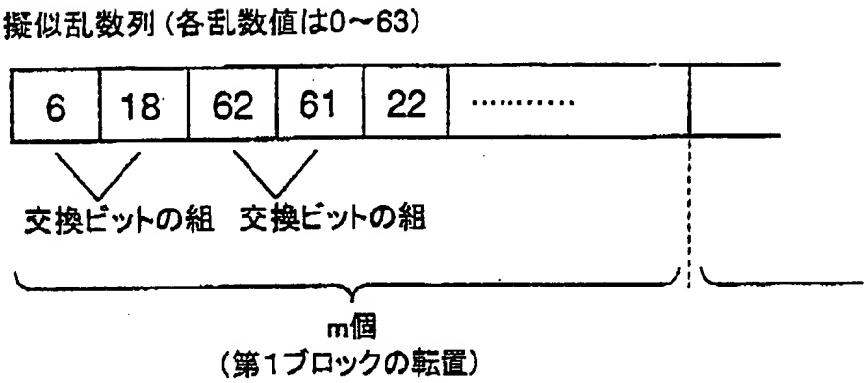
第13図


ビット位置 0 1 2 3 4 5 6 7 8 9 10 11 63
平文
擬似乱数
暗文

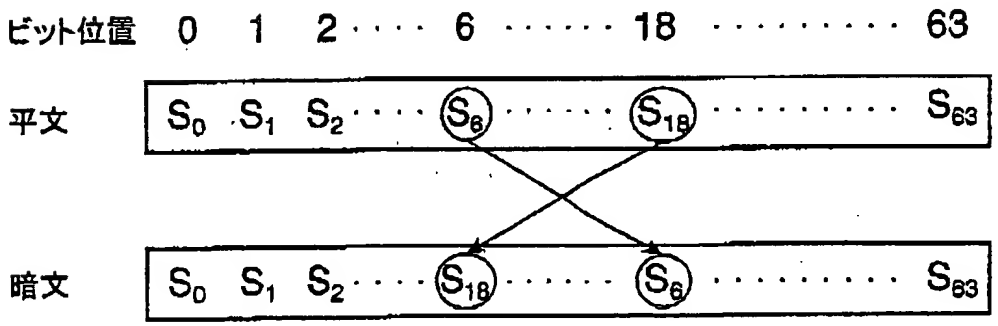
第14図



第 15 図


擬似乱数列（各乱数値は0～63）
6
18
62
61
22
.....
交換ビットの組
交換ビットの組
m個
（第1ブロックの転置）

第 16 図


ビット位置 0 1 2 ・・・・ 6 ・・・・・・ 18 ・・・・・・・・・ 63
平文
S0 S1 S2 ・・・・ S6 ・・・・・・ S18 ・・・・・・・・・ S63
暗文
S0 S1 S2 ・・・・ S18 ・・・・・・ S6 ・・・・・・・・・ S63

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02554

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/18
G09C1/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00
G09C1/00 - 5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Douglas R. Stinson, translated by Koichi Sakurai "Ango Riron no Kiso", Kyoritsu Shuppan, (1996), pp.19-20 (Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	1-13
Y	Douglas R. Stinson, translated by Koichi Sakurai "Ango Riron no Kiso", Kyoritsu Shuppan, (1996), pp.21-24 (Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	1-13
Y	JP, 4-86135, A (Sharp Corporation), 18 March, 1992 (18.03.92), see especially, page 5, lower left column, lines 15-20 (Family: none)	3
Y	Douglas R. Stinson, translated by Koichi Sakurai "Ango Riron no kiso", Kyoritsu Shuppan, (1996), pp.69-72 (Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	5,6

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 July, 2000 (21.07.00)	08 August, 2000 (08.08.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号 PCT/JP00/02554

A. 発明の属する分野の分類（国際特許分類（IPC））
Int.Cl'
H04L9/18
G09C1/04

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int.Cl'
H04L9/00
G09C1/00 - 5/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	Douglas R. Stinson著, 櫻井幸一監訳 「暗号理論の基礎」共立出版, (1996), pp.19-20 (原著: Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	1-13
Y	Douglas R. Stinson著, 櫻井幸一監訳 「暗号理論の基礎」共立出版, (1996), pp.21-24 (原著: Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	1-13

☑ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
21.07.00	08.08.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	丸山 高政 電話番号 03-3581-1101 内線 3576	5W 9570

様式PCT/ISA/210（第2ページ）（1998年7月）

国際調査報告 国際出願番号 PCT/JP00/02554

C (続き). 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 4-86135, A (シャープ株式会社) 18. 3月. 1992 (18. 03. 92), 特に第5頁左下欄第15行～第20行参照, (ファミリーなし)	3
Y	Douglas R. Stinson著, 櫻井幸一監訳 「暗号理論の基礎」共立出版, (1996), pp. 69-72 (原著: Douglas R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, (1995))	5,6